

# WATSON B. LADD

---

(201) 213-9379; watsonbladd@gmail.com

## Education

2013–2018	<b>University of California, Berkeley</b> PhD in Mathematics, May 2018.	Berkeley, CA
2009–2013	<b>University of Chicago</b> BS with Honors in Mathematics. GPA 3.6 (out of 4.0)	Chicago, IL
2005–2009	<b>Academy for the Advancement of Science and Technology</b> High School Diploma June 2009. GPA 3.8 (out of 4.0)	Hackensack, NJ

## Experience

2018–present	<b>Cloudflare</b> Implemented and deployed new public NTP service with first deployment of new security features Spearheaded successful multifunctional effort to deploy advanced security protocols Analyzed applications of cryptographic primitives to business problems	San Francisco, CA
2017	<b>Cloudflare</b> Implemented exported authenticators in an NGINX module	San Francisco, CA
2015, 2016	<b>Mozilla</b> Implemented constant time cryptography for NSS Co-designed and implemented new cryptographic protocol for anonymous advertising (presented at CCS 2016)	San Francisco, CA
2014	<b>Matasano</b> Analyzed novel protocols for security flaws and documented findings Found bugs in SSL implementations related to ECC	Sunnyvale, CA
2013–2018	<b>University of California, Berkeley</b> Teaching discussion sections of calculus, discrete mathematics, and linear algebra courses	Berkeley, CA
2013	<b>Royal Bank of Canada</b> Designed and implemented customized risk reporting tools and analyzed trader performance	New York, NY

## Activities

2013–present	<b>Internet Engineering Task Force</b> Analyse cryptographic protocols considered for new Internet standards	Berkeley, CA
--------------	---	--------------

Discovered security errata in algorithm descriptions

**Awards**  
2013

**Paul R. Cohen Memorial Prize**

Chicago, IL

Awarded annually to the graduating seniors in the field of mathematics who have achieved the highest record in mathematics

**Skills**

Go, C, Rust, and Java programming. NGINX. Cryptography. Kubernetes.